

CLAIMS
(IN CLEAN FORM)

The following claims are the amended claims presented above, in clean form.

1. (Currently Amended) A wireless mobile communication device, comprising:

at least one memory storing a first domain comprising a first set of assets each sharing a first level of trust, and the at least one memory storing a second domain comprising a second set of assets each sharing a second level of trust, wherein the first level of trust is different than the second level of trust; and

a domain controller configured to control the first domain and the second domain, and further configured to control access to the first set of assets and the second set of assets;

wherein the domain controller is further configured to receive a request to perform an operation affecting a particular asset in the first set of assets and to determine whether the request originated from a first entity that has a first trust relationship with the first domain; and

wherein the domain controller is further configured to permit completion of the operation affecting the particular asset only if the request originated from the first entity, and wherein the domain controller is further configured to permit the first entity to perform operations with respect to each of the first set of assets.
2. (Currently Amended) The wireless mobile communication device of claim 1, further comprising a key store for storing cryptographic keys associated with the first

domain, wherein the domain controller is configured to determine whether the first entity is using the cryptographic keys.

3. (Currently Amended) The wireless mobile communication device of claim 1, wherein the domain controller is configured to determine whether the first domain also includes the first entity.

4. (Currently Amended) The wireless mobile communication device of claim 1, wherein the first domain further includes as an asset a software application for which the domain controller permits completion of the operation upon the software application;

wherein completion of the operation is not permitted if the request originated with a second entity that does not have a trust relationship with the first domain.

5. (Currently Amended) The wireless mobile communication device of claim 4, wherein the wireless mobile communication device further comprises a super user software application that has a trust relationship with both the first domain and the second domain.

6. (Currently Amended) The wireless mobile communication device of claim 5, wherein both the first domain and the second domain include the super user software application.

7. (Currently Amended) The wireless mobile communication device of claim 1, wherein the domain controller is further configured to receive information, and to place the information into at least one of the first domain and the second domain.

8. (Currently Amended) The wireless mobile communication device of claim 1, wherein the first set of assets are selected from the group consisting of:

communication pipes, persistent data, properties, and software applications.

9. (Currently Amended) The wireless mobile communication device of claim 1, further comprising a data store for storing properties, wherein the domain controller is further configured to determine whether the operation is permitted by properties in the data store, and to permit completion of the operation if the operation is permitted by the properties in the data store;

wherein completion of the operation is not permitted if the operation is not permitted by the properties in the data store.

10. (Currently Amended) The wireless mobile communication device of claim 9, wherein each property is global, domain-specific, or specific to a particular software application on the wireless mobile communication device.

11. (Currently Amended) A method for secure control of a wireless mobile communication device, comprising:

segregating a plurality assets of the wireless mobile communication device into a first set of assets in a first domain and into a second set of assets in a second domain, wherein the first set of assets includes at least two different types of assets, wherein the first set of assets share a first level of trust to access, wherein the second set of assets share a second level of trust to access, and wherein the first level of trust is different than the second level of trust;

receiving a request from a first entity to perform an operation affecting at least one of the first set of assets;

determining, via a domain controller configured to control the first domain and the second domain, whether the operation is permitted by the first domain, wherein the operation is permitted by the first domain if the first entity has a first trust relationship with the first domain and further wherein the first entity is allowed to perform operations with respect to each of the first set of assets; and

allowing the operation to be completed only if the operation is permitted by the first domain.

12-18. (Canceled)

19. (Currently Amended) The method of claim 11, further comprising the step of:
determining whether the operation is permitted by a property stored at the wireless mobile communication device,

wherein the step of allowing comprises the step of allowing the operation to be completed if the operation is permitted by both the first domain and the property;

wherein the operation is not allowed to be completed if the operation is not permitted by both the first domain and the property, and

wherein the step of determining whether the operation is permitted by the property comprises checking a global property for the wireless mobile communication device and a domain property for the first domain.

20. (Currently Amended) The method of claim 19, wherein the request originates from a software application, and wherein the step of determining whether the operation is permitted further comprises checking an application property for the software application.

21. (Currently Amended) The system of claim 1, wherein the first set of assets includes at least two different assets selected from the group consisting of: communication pipes, persistent data, properties, and software applications.

22. (New) The wireless mobile communications device of claim 1 wherein the domain controller is further configured to deny completion of the operation of the particular asset if the request originated from a second entity that does not have the first trust relationship with the first domain.

23. (New) The wireless mobile communications device of claim 22 wherein the second entity has a second trust relationship with the second domain, and wherein the domain controller is further configured to permit the second entity to perform operations with respect to each of the second set of assets.

24. (New) The method of claim 11 further comprising:
denying completion of the operation if the request originated from a second entity that does not have the first trust relationship with the first domain.

25. (New) The method of claim 22 wherein the second entity has a second trust relationship with the second domain, and wherein the method further comprises:
permitting the second entity to perform operations with respect to each of the second set of assets.

26. (New) A computer readable medium storing program code which, when executed by a processor, performs a method for secure control of a wireless mobile communication device, the method comprising:

segregating a plurality assets of the wireless mobile communication device into a first set of assets in a first domain and into a second set of assets in a second domain, wherein the first set of assets includes at least two different types of assets, wherein the first set of assets share a first level of trust to access, wherein the second set of assets share a second level of trust to access, and wherein the first level of trust is different than the second level of trust;

receiving a request from a first entity to perform an operation affecting at least one of the first set of assets;

determining, via a domain controller configured to control the first domain and the second domain, whether the operation is permitted by the first domain, wherein the operation is permitted by the first domain if the first entity has a first trust relationship with the first domain and further wherein the first entity is allowed to perform operations with respect to each of the first set of assets; and

allowing the operation to be completed only if the operation is permitted by the first domain.

27. (New) The computer readable medium of claim 26, wherein the method performed by the executed program code further comprises:

denying completion of the operation if the request originated from a second entity that does not have the first trust relationship with the first domain.

28. (New) The computer readable medium of claim 27 wherein the second entity has a second trust relationship with the second domain, and wherein the method performed by the executed program code further comprises:

 permitting the second entity to perform operations with respect to each of the second set of assets.